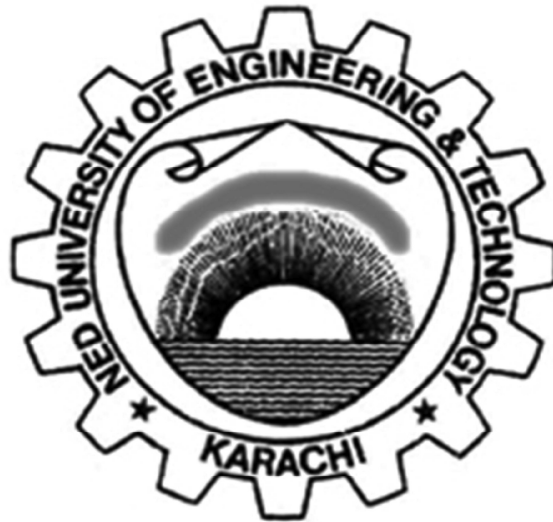


Practical Workbook
CS-426
COMPUTER SYSTEMS SECURITY



Name : _____

Year : _____

Batch : _____

Roll No : _____

Department of Computer & Information Systems Engineering
NED University of Engineering & Technology

Practical Workbook
CS-426
COMPUTER SYSTEMS SECURITY



Prepared by:
Mr. Umar Iftikhar, Ms. Ibshar Ishrat
and Mr. Muhammad Nabeel Ibrahim Khan

Revised in:
February 2021

Revision 01

Department of Computer & Information Systems Engineering
NED University of Engineering & Technology

INTRODUCTION

This workbook has been compiled to assist the conduct of practical classes for CS-426 Computer Systems Security. Practical work relevant to this course aims at providing students a chance to work on hands-on lab sessions for security education , for which SEED Lab sessions funded by NSF has been chosen. SEED lab sessions are now used by thousands of educational institutes worldwide. These lab sessions cover a wide range of topics in computer and information security, including software security, network security, web security, operating system security and mobile app security.

The Course Profile of CS-426 Computer Systems Security lays down the following Course Learning Outcome:

“Demonstrate the use of modern tools and techniques for protecting computer and information systems”

All lab sessions of this workbook have been designed to assist the achievement of the above CLO. A rubric to evaluate student performance has been provided at the end of the workbook.

Lab sessions 1 and 4 provide detailed explanation and experimentation of TCP/IP based attacks. Lab sessions 2 and 3 are related to web security. Lab sessions 5 and 7 are related to software security; namely lab sessions related to the study and exploration of buffer overflow and race condition vulnerability. Lab session 6 is related to SQL Injection attack. Lab session 8 is related to Domain Name Systems (DNS) security. Lab sessions 9, 10 and 11 provide a comprehensive framework for exploring information security (encryption). Lab sessions 12 and 13 explore Linux firewalling capabilities. All of the above mentioned lab sessions will be conducted on Linux based virtual machine provided by SEED project.

CONTENTS

Lab Session No.	Title	Page No.	Teacher's Signature	Date
1	Practice Packet Sniffing and Spoofing	1		
2	Examine Cross-Site Scripting (XSS) Attack	8		
3	Explore Web tracking	15		
4	Examine Attacks on TCP/IP Protocols	24		
5	Simulate Buffer Overflow Vulnerability	31		
6	Explore SQL injection attack	39		
7	Explore Race Condition Vulnerability	48		
8	Practice Local DNS Attack	54		
9	Carry out Crypto - Secret Key Encryption	62		
10	Carry out Crypto - One-Way Hash Function and MAC	68		
11	Carry out Crypto - Public-Key Cryptography and PKI	71		
12	Explore Firewall under suitable environment	78		
13	Explore Web Proxy in Firewall	83		
14	Complex Engineering Activity	93		
15	Rubrics	95		